Finite Fields and Their Applications 18 (2012) 728–737

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On a conjecture of polynomials with prescribed range

Amela Muratović-Ribić [a], Qiang Wang [b,*,1]

[a] University of Sarajevo, Department of Mathematics, Zmaja od Bosne 33-35, 71000 Sarajevo, Bosnia and Herzegovina
[b] School of Mathematics and Statistics, Carleton University, Ottawa, Ontario K1S 5B6, Canada

ARTICLE INFO

Article history:
Received 18 March 2011
Revised 24 January 2012
Accepted 27 February 2012
Available online 16 March 2012
Communicated by Rudolf Lidl

MSC:
11T06

Keywords:
Polynomials
Prescribed range

ABSTRACT

We show that, for any integer m with $3 < m \leqslant \min\{p-1, q/2\}$ where $q = p^n > 9$ there exists a multiset M satisfying that $0 \in M$ has the highest multiplicity $q-m$ and $\sum_{b\in M} b = 0$ such that every polynomial over the finite field $\mathbb{F}_q$ with the prescribed range M has degree greater than $q-m$. This implies that Conjecture 5.1 in Gács et al. (2010) [6] is false over any finite field $\mathbb{F}_q$ for $p > 9$ and $k := m-1 \geqslant 3$.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of $q = p^n$ elements and $\mathbb{F}_q^*$ be the set of all nonzero elements. Any mapping from $\mathbb{F}_q$ to itself can be uniquely represented by a polynomial of degree at most $q-1$. The degree of such a polynomial is called the *reduced* degree. A *value set* of a polynomial f over $\mathbb{F}_q$ is the set V_f of images when view f as a mapping from $\mathbb{F}_q$ to itself. The polynomial f is a permutation polynomial (PP) of $\mathbb{F}_q$ if and only if the size $|V_f| = q$. The distribution of value sets of polynomials has been studied in [3]. A lot of effort has been made in finding lower and upper bounds of $|V_f|$ if f is not a PP, see for example, [4,7,10,12–14]. One of the most known results in this area was due to Wan [13], who proved $|V_f| \leqslant q - \lceil (q-1)/n \rceil$, which was first conjectured by Mullen [10]. Polynomials with prescribed sizes of values sets such as *minimal value set polynomials* (that are polynomials f over $\mathbb{F}_q$ with degree n satisfying $|V_f| = \lceil q/n \rceil$) have been studied in [2,5]. The complete classification of

* Corresponding author.
E-mail addresses: amela@pmf.unsa.ba (A. Muratović-Ribić), wang@math.carleton.ca (Q. Wang).

[1] Research is partially supported by NSERC of Canada.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2012.02.004

minimal value set polynomials over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ is done in [11] and it is still open for the general extension fields. All these results related $|V_f|$ with the degree n of the polynomial.

Let us also consider multiplicities of elements in the value sets of polynomials. A multiset M of size q of field elements is called the *range* of the polynomial $f(x) \in \mathbb{F}_q[x]$ if $M = \{f(x)\colon\ x \in \mathbb{F}_q\}$ as a multiset (that is, not only values, but also multiplicities need to be the same). Here we use the set notation for multisets as well. Biró [1] described polynomials whose range is a multiset with only two distinct nonzero values. A nice reveal of connections among a combinatorial number theoretical result, polynomials of prescribed ranges and hyperplanes in vector spaces over finite fields can be found in [6], which we refer it to the readers for more details. In their study of polynomials with prescribed range, Gács et al. recently proposed the following conjecture on the ranges of polynomials and their degrees.

Conjecture 1. *(See [6, Conjecture 5.1].) Suppose $M = \{a_1, a_2, \ldots, a_q\}$ is a multiset of $\mathbb{F}_q$ with $a_1 + \cdots + a_q = 0$, where $q = p^n$, p prime. Let $k < \sqrt{p}$. If there is no polynomial with range M of degree less than $q - k$, then M contains an element of multiplicity at least $q - k$.*

We note that Conjecture 1 is equivalent to

Conjecture 2. *Suppose $M = \{a_1, a_2, \ldots, a_q\}$ is a multiset of $\mathbb{F}_q$ with $a_1 + \cdots + a_q = 0$, where $q = p^n$, p prime. Let $k < \sqrt{p}$. If multiplicities of all elements in M are less than $q - k$, then there exists a polynomial with range M of the degree less than $q - k$.*

In the case $k = 2$, Conjecture 1 holds by Theorem 2.2 in [6]. In particular, Theorem 2.2 in [6] gives a complete description of M so that there is no polynomial with range M of reduced degree less than $q - 2$. In this paper, we study the above conjecture for $k \geqslant 3$.

Suppose we take a prescribed range M such that the highest multiplicity in M is $q - k - 1$. If the above conjecture were true then it follows that there exists a polynomial, say $g(x)$, with range M and the degree of $g(x)$ is less than $q - k$. On the other hand, if $a \in M$ is the element with multiplicity $q - k - 1$ then the polynomial $g(x) - a$ has $q - k - 1$ roots and thus the degree of $g(x)$ is at least equal to the highest multiplicity $q - k - 1$ in M. Therefore the degree of $g(x)$ must be $q - k - 1$. This means that, if Conjecture 2 were true, then for every multiset M with the highest multiplicity $q - k - 1$ where $1 \leqslant k < \sqrt{p}$ there exists a polynomial with range M of the degree $q - k - 1$.

Let $M = \{a_1, a_2, \ldots, a_q\}$ be a given multiset. We consider polynomials $f(x) : \mathbb{F}_q \to M$, with the least degree. Let $q - k - 1$ be the highest multiplicity in M. If $a \in M$ is an element with multiplicity $q - k - 1$ then the polynomial $f(x) - a$ has the same degree as $f(x)$ and 0 is in the range of $f(x) - a$ such that 0 has the same highest multiplicity $q - k - 1$. Therefore, we will consider only multisets M where 0 has the highest multiplicity for the rest of the article.

In particular, we prove the following theorem.

Theorem 1. *Let $\mathbb{F}_q$ be a finite field of $q = p^n$ elements with $q > 9$. For every m with $3 < m \leqslant \min\{p - 1, q/2\}$ there exists a multiset M with $\sum_{b \in M} b = 0$ and the highest multiplicity $q - m$ achieved at $0 \in M$ such that every polynomial over the finite field $\mathbb{F}_q$ with the prescribed range M has degree greater than $q - m$.*

In particular, for any $p > 9$ and $3 \leqslant k < \sqrt{p}$, if we take $m = k + 1$, i.e., $3 < m < \sqrt{p} + 1 \leqslant \min\{p - 1, q/2\}$, then Theorem 1 implies that Conjecture 2 fails.

2. Proof of Theorem 1

Let m be a fixed positive integer such that $3 < m \leqslant \min\{p - 1, q/2\}$. Because $q > 9$, such m exists. Let M be a multiset such that $0 \in M$ has the highest multiplicity $q - m$ and $\sum_{b \in M} b = 0$. We note that the multiplicity of any nonzero element in $M \leqslant q/2$ and the highest multiplicity $q - m \geqslant q/2$ is indeed achieved at 0. Consider the polynomial $f : \mathbb{F}_q \to M$. Let $U \subseteq \mathbb{F}_q$ such that $f(U) = \{0^{q-m}\}$ (the multiset of $q - m$ zeros) and $T = \mathbb{F}_q \setminus U$, i.e., $x \in T$ implies $f(x) \neq 0$. Then $|U| = q - m$ and $|T| = m$ and

$M = f(U) \cup f(T)$. Then a polynomial $f : \mathbb{F}_q \to M$ can be written in the form $f(x) = h(x)P(x)$ where $P(x) = \prod_{s\in U}(x-s)$ and $h(x) \neq 0$ has no zeros in T. Then $\deg(f) \geqslant \deg(P) = q-m$. We note that there is a bijection between polynomials of reduced degree with range $M = \{a_1, \ldots, a_q\}$ and the ordered sets $(b_1, \ldots, b_q)$ (that is, permutations) of $\mathbb{F}_q$: a permutation corresponds to the function $f(b_i) = a_i$. For each U, there are many different $h(x)$'s corresponding to different ordered sets $(b_1, \ldots, b_q)$ such that $f(b_i) = 0$ for all $b_i \in U$. However, if $h(x) = \lambda \in \mathbb{F}_q^*$ then $f(x)$ is a polynomial of the least degree and each polynomial $f(x)$ is uniquely determined by a set T and a nonzero scalar λ.

Thus we denote $f(x)$ by

$$f_{(\lambda,T)}(x) = \lambda \prod_{s\in\mathbb{F}_q\setminus T} (x-s). \tag{1}$$

Therefore its range M is also uniquely determined by T and λ. Denote by $\mathcal{T}$ the family of all subsets of $\mathbb{F}_q$ of cardinality m, i.e.,

$$\mathcal{T} = \big\{T \;\big|\; T \subseteq \mathbb{F}_q,\ |T| = m\big\}.$$

Denote by $\mathcal{M}$ the family of all multisets M of order q containing 0, having the highest multiplicity $q-m$ achieved at 0 and whose sum of elements in M is equal to the 0, i.e.,

$$\mathcal{M} = \left\{M \;\middle|\; 0 \in M,\ \text{multiplicity}(0) = q-m,\ \sum_{b\in M} b = 0\right\}.$$

Eq. (1) uniquely determines a mapping

$$\mathcal{F} : \mathbb{F}_q^* \times \mathcal{T} \to \mathcal{M}$$

where

$$(\lambda, T) \mapsto \text{range}\big(f_{\lambda,T}(x)\big).$$

Also, the condition $q-m < q-3$ implies that $\deg(f_{\lambda,T}) < q-1$. Now by Eq. (1) it follows that for every $\hat{s} \in T$ we have

$$f_{\lambda,T}(\hat{s}) = \lambda P(\hat{s}) = \lambda \prod_{s\in\mathbb{F}_q,\, s\neq\hat{s}} (\hat{s}-s)\left(\prod_{s\in T,\, s\neq\hat{s}} (\hat{s}-s)\right)^{-1} = -\lambda\left(\prod_{s\in T,\, s\neq\hat{s}} (\hat{s}-s)\right)^{-1}. \tag{2}$$

(Note that this equation does not hold for $\hat{s} \in \mathbb{F}_q \setminus T$.) In the following we find an upper bound of $|\text{range}(\mathcal{F})|$ and a lower bound of $|\mathcal{M}|$ and show that $|\mathcal{M}| > |\text{range}(\mathcal{F})|$. This implies that Theorem 1 holds. Further, we will use notation $cT + b = \{ct + b \mid t \in T\}$.

First of all we observe

Lemma 1. *Let λ and T be given. For any $c \in \mathbb{F}_q^*$ and any $b \in \mathbb{F}_q$, we have*

$$f_{(\lambda,T)}(\hat{s}) = f_{(c^{m-1}\lambda, cT+b)}(c\hat{s}+b), \quad \textit{for } \hat{s} \in T$$

i.e.,

$$\mathcal{F}(\lambda, T) = \mathcal{F}\big(c^{m-1}\lambda, cT + b\big).$$

Proof. Substituting in (2), we obtain $f_{(c^{m-1}\lambda,cT+b)}(c\hat{s}+b) = -c^{m-1}\lambda(\prod_{s\in T,\ s\neq\hat{s}}((c\hat{s}+b)-(cs+b)))^{-1} = -\lambda(\prod_{s\in T,\ s\neq\hat{s}}(\hat{s}-s))^{-1} = f_{(\lambda,T)}(\hat{s})$. □

In order to find an upper bound of the cardinality of range($\mathcal{F}$), we recall Burnside's Lemma (see [9, p. 95]).

Theorem 2 *(Burnside's Lemma). Let G be a permutation group acting on a set X. For $g \in G$ let $\psi(g)$ denote the number of points of X fixed by g. Then the number of orbits of G is equal to $\frac{1}{|G|}\sum_{g\in G}\psi(g)$.*

Now we obtain an upper bound of the cardinality of range($\mathcal{F}$).

Lemma 2. *Let $m < p$, $d = \gcd(q-1, m-1)$ and $\phi(i)$ be the Euler totient function. Then*

$$\left|\text{range}(\mathcal{F})\right| \leqslant \frac{(q-1)(q-2)\dots(q-m+1)}{m!} + \sum_{\substack{i\mid d\\ i>1}} \phi(i)\binom{\frac{q-1}{i}}{\frac{m-1}{i}}.$$

Proof. Let $\mathcal{G}$ be group of all non-constant linear polynomials in $\mathbb{F}_q[x]$ with the composition operation. Then $\mathcal{G}$ acts on the set $\mathbb{F}_q^* \times \mathcal{T}$ with $\Phi : \mathcal{G} \times (\mathbb{F}_q^* \times \mathcal{T}) \to \mathbb{F}_q^* \times \mathcal{T}$, where

$$\Phi : \big(cx+b, (\lambda, T)\big) \mapsto \big(c^{m-1}\lambda, cT+b\big).$$

The elements of the same orbit

$$\mathcal{G}(\lambda, T) = \big\{\big(c^{m-1}\lambda, cT+b\big) \bigm| cx+b \in \mathcal{G}\big\}$$

are all mapped to the same element $M \in \mathcal{M}$ by Lemma 1. By Burnside's Lemma the number of orbits N is given by

$$N = \frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}} \left|\left(\mathbb{F}_q^* \times \mathcal{T}\right)_g\right|,$$

where $g(x) = cx+b$, and

$$\left(\mathbb{F}_q^* \times \mathcal{T}\right)_g = \big\{(\lambda, T) \bigm| (\lambda, T) \in \mathbb{F}_q^* \times \mathcal{T},\ \big(c^{m-1}\lambda, cT+b\big) = (\lambda, T)\big\}.$$

The equation $cx+b = x$ over $\mathbb{F}_q$ is equivalent to $(c-1)x = -b$, which has exactly one solution if $c \neq 1$; no solutions if $c = 1$ and $b \neq 0$; q solutions if $c = 1$ and $b = 0$. If $c \neq 1$ and $i := ord(c) \mid q-1$, then this linear polynomial has one fixed element and $\frac{q-1}{i}$ cycles of length i. Indeed, $f^k(x) = c^k x + b(c^{k-1} + \dots + c + 1) = c^k x + b\frac{c^k-1}{c-1}$. Thus $f^i(x) = x$ for all $x \in \mathbb{F}_q \setminus \{b(1-c)^{-1}\}$, and $x \neq f^k(x)$ for $1 \leqslant k < i$. If $c = 1$ and $b \neq 0$ then $g^p(x) = x + pb = x$ and thus $g(x)$ has cycles of length p since $p = char(\mathbb{F}_q)$.

Assume $T = cT + b$. Let $s \in T$. Then $g(s) \in cT + b = T$. So the cycle $(s, g(s), g^2(s), \dots, g^i(s) = s)$ is contained in T.

This means that, under the assumptions of $c \neq 1$ and $T = cT + b$, either T has one fixed element and $\frac{m-1}{i}$ cycles of the length i which are defined by permutation $g(x)$, or T has $\frac{m}{i}$ cycles of the length i which are defined by permutation $g(x)$. In the latter case, the fixed element of $g(x)$ is in $\mathbb{F}_q \setminus T$.

In the former case, if $c \in \mathbb{F}_q^* \setminus \{1\}$ satisfies $i = ord(c) \mid d = \gcd(q-1, m-1)$ then there are $\binom{\frac{q-1}{i}}{\frac{m-1}{i}}$ sets fixed by $g(x)$. Moreover, $c^{m-1} = (c^i)^{\frac{m-1}{i}} = 1$. Hence, for each set T fixed by $g(x)$ and any $\lambda \in \mathbb{F}_q^*$ we must have $(c^{m-1}\lambda, cT + b) = (\lambda, T)$. This implies that

$$\left|\left(\mathbb{F}_q^* \times \mathcal{T}\right)_g\right| = (q-1)\binom{\frac{q-1}{i}}{\frac{m-1}{i}}.$$

If $c \in \mathbb{F}_q^* \setminus \{1\}$ satisfies $i = ord(c) \mid \gcd(q-1, m)$ then there are $\binom{\frac{q-1}{i}}{\frac{m}{i}}$ sets T fixed by $g(x)$. But for each T fixed by $g(x)$, $c^{m-1} = c^{-1} \neq 1$ and thus $(c^{m-1}\lambda, cT + b) \neq (\lambda, T)$. Therefore

$$\left|\left(\mathbb{F}_q^* \times \mathcal{T}\right)_g\right| = 0.$$

If $c = 1$ and $b = 0$ then $g(x) = x$. So $|(\mathbb{F}_q^* \times \mathcal{T})_g| = (q-1)\binom{q}{m}$. If $c = 1$ and $b \neq 0$ then $cT + b \neq T$. Otherwise, it implies that T contains elements of the cycles of the length p which contradicts to $m < p$.

Since $d = \gcd(q-1, m-1)$, we obtain

$$\begin{aligned}
N &= \frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}}\left|\left(\mathbb{F}_q^* \times \mathcal{T}\right)_g\right| \\
&= \frac{1}{q(q-1)}\left((q-1)\cdot\binom{q}{m} + \sum_{\substack{c\in\mathbb{F}_q^*\setminus\{1\}\\ i=ord(c)\mid d\\ b\in\mathbb{F}_q}}(q-1)\binom{\frac{q-1}{i}}{\frac{m-1}{i}}\right) \\
&= \frac{1}{q(q-1)}\left((q-1)\cdot\binom{q}{m} + q(q-1)\sum_{\substack{c\in\mathbb{F}_q^*\setminus\{1\}\\ i=ord(c)\mid d}}\binom{\frac{q-1}{i}}{\frac{m-1}{i}}\right) \\
&= \frac{(q-1)(q-2)\ldots(q-m+1)}{m!} + \sum_{i>0,\ i\mid d}\phi(i)\binom{\frac{q-1}{i}}{\frac{m-1}{i}},
\end{aligned}$$

where $\phi(i)$ is the number of c's such that the order of c is $i > 1$. Since two orbits could possibly be mapped to the same multiset $M \in \mathcal{M}$ we finally have an inequality

$$\left|\text{range}(\mathcal{F})\right| \leqslant \frac{(q-1)(q-2)\ldots(q-m+1)}{m!} + \sum_{i>0,\ i\mid d}\phi(i)\binom{\frac{q-1}{i}}{\frac{m-1}{i}}. \qquad \square \tag{3}$$

Next we find a lower bound of the cardinality of

$$\mathcal{M} = \left\{M = \{\overbrace{0, 0, \ldots, 0}^{q-m \text{ times}}, b_1, b_2, \ldots, b_m\},\ b_i \neq 0,\ i = 1, 2, \ldots, m,\ \sum_{i=1}^{m} b_i = 0\right\}.$$

Thus, we need to find the number of multisets $\{b_1, \ldots, b_m\}$ such that $b_i \neq 0$ for $i = 1, \ldots, m$ and

$$b_1 + b_2 + \cdots + b_m = 0. \tag{4}$$

Although we can find a simpler exact formula for the number of solutions to Eq. (4), we prefer the following lower bound for $|\mathcal{M}|$ which has the same format as the upper bound of $|\mathrm{range}(\mathcal{F})|$ in order to compare them directly.

Lemma 3. *Let $A = 1$ if $m-1 \mid q-1$ and $A = 0$ otherwise. If $p > m \geqslant 6$ then*

$$|\mathcal{M}| \geqslant \frac{(q-1)\dots(q-m+2)(q-2)}{m!} + \sum_{\substack{1<i<m-1 \\ i \mid \gcd(q-1,m-1)}} \frac{q-1}{q}\left[\binom{q-1}{\frac{m-1}{i}} + (-1)^{\frac{m-1}{i}}\right] + A(q-1).$$

If $m = 4$ then

$$|\mathcal{M}| \geqslant \frac{(q-1)(q-2)^2}{4!}.$$

If $m = 5$ then

$$|\mathcal{M}| \geqslant \frac{(q-1)(q-2)^2(q-3)}{5!} + A(q-1).$$

Proof. In order to give a lower bound of $|\mathcal{M}|$, we count two different classes of families of multisets M. The first class contains families of those multisets M such that all nonzero elements b_i's have the same multiplicities greater than one except the last element b_m. And the second family class contains those multisets M such that if we do not consider b_{m-1} and b_m, then all other elements b_i have multiplicity one. First, we count those multisets M such that all nonzero elements b_i's have the same multiplicities greater than one except the last element b_m. That is, for any i such that $1 < i < m-1$ and $i \mid \gcd(q-1, m-1)$, we want to choose $\frac{m-1}{i}$ pairwise distinct nonzero elements b_j's, each of multiplicity i, so that $\sum_{j=1}^{\frac{m-1}{i}} ib_j \neq 0$ (the sum being equal to zero would imply $b_m = 0$, a contradiction). For each such i, we denote the family of these multisets by $\mathcal{M}_i$.

We note that each multiset $M \in \mathcal{M}_i$ can be written as

$$M = \{\overbrace{0, 0, \dots, 0}^{q-m \text{ times}}, \overbrace{b_1, \dots, b_1}^{i \text{ times}}, \dots, \overbrace{b_{\frac{m-1}{i}}, \dots, b_{\frac{m-1}{i}}}^{i \text{ times}}, b_m\}.$$

Obviously each multiset is invariant to the ordering of the elements $b_1, \dots, b_{\frac{m-1}{i}}$. By [8, Theorem 1.2], the number of sets with pairwise distinct nonzero elements $b_1, \dots, b_{\frac{m-1}{i}}$ such that $\sum_{j=1}^{\frac{m-1}{i}} b_j \neq 0$ is

$$\sum_{b \in \mathbb{F}_q^*} N\left(\frac{m-1}{i}, b, \mathbb{F}_q^*\right) = \frac{q-1}{q}\left[\binom{q-1}{\frac{m-1}{i}} + (-1)^{\frac{m-1}{i}}\right]$$

and thus

$$|\mathcal{M}_i| = \frac{q-1}{q}\left[\binom{q-1}{\frac{m-1}{i}} + (-1)^{\frac{m-1}{i}}\right].$$

Similarly, if $m-1 \mid q-1$, we denote by $\mathcal{M}_{m-1}$ the set of multisets M such that all b_i's are the same nonzero element for $i = 1, \ldots, m-1$ and their sum together with b_m is zero. It is easy to see that there are $q-1$ such M's, i.e., $|\mathcal{M}_{m-1}| = q-1$.

Now we show that $\mathcal{M}_i \cap \mathcal{M}_j = \emptyset$ for $1 < i \neq j \leqslant m-1$. We prove this by contradiction and we use heavily the fact that, for each i, there are $\frac{m-1}{i}+1$ distinct elements in $M \in \mathcal{M}_i$ if $b_m \neq b_k$ for $1 \leqslant k \leqslant \frac{m-1}{i}$ and there are $\frac{m-1}{i}$ distinct elements in M if $b_m = b_k$ for some k. Assume that $\mathcal{M}_i \cap \mathcal{M}_j \neq \emptyset$. Obviously, $\frac{m-1}{i} \neq \frac{m-1}{j}$ because $i \neq j$. Hence either $\frac{m-1}{i}+1 = \frac{m-1}{j}$ or $\frac{m-1}{j}+1 = \frac{m-1}{i}$. Assume that $M \in \mathcal{M}_i \cap \mathcal{M}_j$ for some $j < i \leqslant m-1$. Then $\frac{m-1}{i}+1 = \frac{m-1}{j}$. This implies that, in the multiset M, we have $\frac{m-1}{i}$ elements of multiplicity i and one element of multiplicity 1 since $M \in \mathcal{M}_i$. Moreover, the number of elements of multiplicity j is $\frac{m-1}{j}-1$ and there is one element of multiplicity $j+1$ since $M \in \mathcal{M}_j$. Because $i > j$, we must have $i = j+1$ and $j = 1$ by comparing the multiplicities. However, this implies we must have $\frac{m-1}{i} = 1$ and $\frac{m-1}{j}-1 = 1$. Hence $i = m-1$ and $j = \frac{m-1}{2}$, contradicts to that $i = j+1$ for $m > 3$. Therefore $\mathcal{M}_i \cap \mathcal{M}_j \neq \emptyset$ for all $1 < i \neq j \leqslant m-1$. Now for $m \geqslant 4$ we have

$$\left| \bigcup_{\substack{1<i\leqslant m-1 \\ i \mid \gcd(q-1,m-1)}} \mathcal{M}_i \right| = A(q-1) + \sum_{\substack{1<i<m-1 \\ i \mid \gcd(q-1,m-1)}} \frac{q-1}{q}\left[\binom{q-1}{\frac{m-1}{i}} + (-1)^{\frac{m-1}{i}}\right].$$

Next we count those multisets M such that all nonzero elements b_i's have multiplicities one if we do not consider the last two elements b_{m-1}, b_m. That is, $b_1, \ldots, b_{m-2}$ are pairwise distinct nonzero elements, $b_{m-1} \neq 0$ is chosen in a way such that $\sum_{j=1}^{m-1} b_j \neq 0$, and b_m is uniquely determined by $\sum_{j=1}^{m} b_j = 0$. Elements b_{m-1} and b_{m-2} can be equal to some of the elements previously chosen. The family of such multisets is denoted by $\mathcal{M}_0$. Since that b_{m-1} and b_m could be same as one of b_j's where $j = 1, \ldots, m-2$, the highest multiplicity could be at most 3.

Consider all $(q-1)\ldots(q-m+2)$ different ordered tuples $(b_1, \ldots, b_{m-2})$. If $-\sum_{j=1}^{m-2} b_j \neq 0$ we can choose b_{m-1} in $q-2$ ways and otherwise there are $q-1$ choices for b_{m-1}. Thus in total there are at least $(q-1)\ldots(q-m+2)(q-2)$ ordered tuples $(b_1, \ldots, b_m)$.

Let S_1 be the number of such ordered tuples with all elements pairwise distinct, S_2 be the number of ordered tuples with $m-2$ elements of the multiplicity one and one elements of the multiplicity two, S_3 be the number of tuples with exactly two elements of the multiplicity two and all other elements of the multiplicity one, and S_4 be the number of tuples with exactly one element of the multiplicity three and all other elements of the multiplicity one. Because multisets are invariant to the ordering, there are at least

$$\frac{S_1}{m!} + \frac{S_2}{(m-1)!} + \frac{S_3}{(m-2)!2!} + \frac{S_4}{(m-2)!} \geqslant \frac{(q-1)\ldots(q-m+2)(q-2)}{m!}$$

such multisets in $\mathcal{M}_0$, i.e.,

$$|\mathcal{M}_0| \geqslant \frac{(q-1)\ldots(q-m+2)(q-2)}{m!}.$$

We note that each multiset from $\mathcal{M}_0$ contains at least $m-2$ distinct elements and each multiset from $\mathcal{M}_i$ with $i > 1$ contains at most $\frac{m-1}{i}+1 \leqslant \frac{m-1}{2}+1$ distinct elements. Since $\frac{m-1}{2}+1 < m-2$ for $m \geqslant 6$ we have that $\mathcal{M}_0 \cap \mathcal{M}_i = \emptyset$ as long as $m \geqslant 6$. Therefore we can conclude that for $m \geqslant 6$ we have

$$|\mathcal{M}| \geqslant |\mathcal{M}_0| + \left| \bigcup_{\substack{1<i\leqslant m-1 \\ i \mid \gcd(q-1,m-1)}} \mathcal{M}_i \right| \geqslant \frac{(q-1)\ldots(q-m+2)(q-2)}{m!}$$

$$+ \sum_{\substack{1<i<m-1 \\ i \mid \gcd(q-1,m-1)}} \frac{q-1}{q}\left[\binom{q-1}{\frac{m-1}{i}} + (-1)^{\frac{m-1}{i}}\right] + A(q-1).$$

Let $m = 4$. Then

$$|\mathcal{M}| \geqslant |\mathcal{M}_0| \geqslant \frac{(q-1)(q-2)(q-2)}{4!}.$$

If $m = 5$, then $i > 1$ and $i \mid \gcd(4, q-1)$ imply $i = 2$ or $i = 4$. Obviously $\mathcal{M}_0 \cap \mathcal{M}_4 = \emptyset$ because each element in a multiset of $\mathcal{M}_0$ has multiplicity at most 3. Now we have

$$|\mathcal{M}| \geqslant |\mathcal{M}_0| + |\mathcal{M}_4| = \frac{(q-1)(q-2)(q-3)(q-2)}{5!} + A(q-1). \qquad \square$$

We need the following simple result to compare the bounds of $\mathcal{M}$ and $|\mathrm{range}(\mathcal{F})|$ in order to complete the proof of Theorem 1.

Lemma 4.

(i) *For $m \geqslant 4$, we have*

$$\frac{(q-1)(q-2)\ldots(q-m+1)}{m!} < \frac{(q-1)\ldots(q-m+2)(q-2)}{m!}.$$

(ii) *If $1 < i < m-1$, $m \geqslant 4$ and $i \mid \gcd(q-1, m-1)$ then*

$$\phi(i)\binom{\frac{q-1}{i}}{\frac{m-1}{i}} < \frac{q-1}{q}\left[\binom{q-1}{\frac{m-1}{i}} + (-1)^{\frac{m-1}{i}}\right],$$

where $\phi(i)$ denotes Euler's totient function.

(iii) *If $i = m-1 \mid q-1$, then*

$$\phi(m-1)\binom{\frac{q-1}{i}}{\frac{m-1}{i}} < q-1,$$

where $\phi(m)$ denotes Euler's totient function.

Proof. (i) Clearly, $q-m+1 < q-2$ for $m \geqslant 4$.

(ii) Using $\phi(i) < i$, $-1 \leqslant (-1)^{\frac{m-1}{i}} \leqslant 1$ and $\frac{qi}{q-1}\left(\frac{\frac{q-1}{i}}{\frac{m-1}{i}}\right) > 1$, to prove (ii) it is enough to prove

$$2\frac{q}{q-1}i\binom{\frac{q-1}{i}}{\frac{m-1}{i}} < \binom{q-1}{\frac{m-1}{i}},$$

which follows from $\frac{q-1}{i} - k < q-1-k$ for $k = 3, 4, \ldots, \frac{m-1}{i} - 1$ and

$$\frac{2qi}{q-1}\left(\frac{q-1}{i}\left(\frac{q-1}{i} - 1\right)\right) < (q-1)(q-2).$$

Indeed, the last inequality reduces to $0 < (i-2)q^2 - (i-2)q + 2i$, which trivially holds for all q.

(iii) If $i = m-1 \mid q-1$ then $\phi(m-1)\frac{q-1}{m-1} < q-1$. $\square$

Proof of Theorem 1. If $p > m \geqslant 6$ it follows directly from Lemmas 2, 3, 4.

If $m = 5$, $m < p$ implies $p \geqslant 7$. Then for $q > 9$ we have

$$\begin{aligned}\big|\mathrm{range}(\mathcal{F})\big| &\leqslant \frac{(q-1)(q-2)(q-3)(q-4)}{5!} + \phi(2)\binom{\frac{q-1}{2}}{2} + A\phi(4)\frac{q-1}{4}\\ &= \frac{(q-1)(q-2)(q-3)(q-4)}{5!} + \frac{(q-1)(q-3)}{8} + A\frac{q-1}{2}\\ &\leqslant \frac{(q-1)(q-2)(q-3)(q-2)}{5!} + A(q-1)\\ &\leqslant |\mathcal{M}|.\end{aligned}$$

If $m = 4$ and $3 \nmid q-1$ then the result follows directly from Lemmas 2, 3, and 4(i). If $3 \mid q-1$ then

$$\big|\mathrm{range}(\mathcal{F})\big| \leqslant \frac{(q-1)(q-2)(q-3)}{4!} + \phi(3)\frac{q-1}{3} < \frac{(q-1)(q-2)^2}{4!} < |\mathcal{M}|$$

holds for $q > 18$. Note that $m \leqslant p$ implies $p \geqslant 5$. The only possible prime power $9 < q \leqslant 18$ such that $p \geqslant 5$ and $3 \mid q-1$ is $q = 13$. It is easy to compute that the number of all the possible solutions to Eq. (4) with desired properties over $\mathbb{F}_{13}$ is $|\mathcal{M}| = 105$ by a computer program. For $q = 13$, then $\gcd(q-1, m-1) = 3$ and thus $|\mathrm{range}(\mathcal{F})| \leqslant 63 < 105 = |\mathcal{M}|$. Hence the proof is complete. □

If $m = 2$ and $m = 3$ these polynomials satisfying the conjecture do exist. Indeed, if $m = 2$ and $b_2 = -b_1$, then we can construct the minimum degree polynomial $f(x) = \lambda\prod_{s\in\mathbb{F}_q\setminus T}(x-s)$ with the prescribed range $M = \{0, \ldots, 0, b_1, -b_1\}$ by letting $T = \{b_1^{-1}, 0\}$ and $\lambda = 1$.

For the case $m = 3$, for any multiset $M = \{0, \ldots, 0, b_1, b_2, b_3\}$ with $b_1 + b_2 + b_3 = 0$ such that b_1, b_2, b_3 are all nonzero there exists a polynomial $f(x) = \lambda\prod_{s\in\mathbb{F}_q\setminus T}(x-s)$ of the least degree with range M. Indeed, let $T = \{b_2, -b_1, 0\}$ and $\lambda = b_1b_2b_3$. Then using $b_3 = -(b_1+b_2)$ we obtain $f(b_2) = b_1b_2b_3\frac{-1}{(b_2+b_1)b_2} = b_1$, $f(-b_1) = b_1b_2b_3\frac{-1}{(-b_1-b_2)(-b_1)} = b_2$, and $f(0) = b_1b_2b_3\frac{-1}{(b_1)(-b_2)} = b_3$.

Acknowledgments

We thank referees for their helpful suggestions.

References

[1] A. Biró, On polynomials over prime fields taking only two values on the multiplicative group, Finite Fields Appl. 6 (2000) 302–308.
[2] L. Carlitz, D.J. Lewis, W.H. Mills, E.G. Straus, Polynomials over finite fields with minimal value sets, Mathematika 8 (1961) 121–130.
[3] S.D. Cohen, The distribution of polynomials over finite fields, Acta Arith. 17 (1970) 255–271.
[4] P. Das, G.L. Mullen, Value sets of polynomials over finite fields, in: Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Oaxaca, 2001, Springer, Berlin, 2002, pp. 80–85.
[5] J. Gomez-Calderon, D.J. Madden, Polynomials with small value set over finite fields, J. Number Theory 28 (2) (1988) 167–188.
[6] A. Gács, T. Héger, Z.L. Nagy, D. Pálvölgyi, Permutations, hyperplanes and polynomials over finite fields, Finite Fields Appl. 16 (2010) 301–314.
[7] R. Guralnick, D. Wan, Bounds for fixed point free elements in a transitive group and applications to curves over finite fields, Israel J. Math. 101 (1997) 255–287.
[8] J. Li, D. Wan, On the subset sum problem over finite fields, Finite Fields Appl. 14 (2008) 911–929.
[9] J.H. van Lint, R.M. Wilson, A Course in Combinatorics, Cambridge University Press, 2001.
[10] G.L. Mullen, Permutation polynomials over finite fields, in: Finite Fields, Coding Theory, and Advances in Communications and Computing, Las Vegas, NV, 1991, in: Lect. Notes Pure Appl. Math., vol. 141, Dekker, New York, 1993, pp. 131–151.
[11] W.H. Mills, Polynomials with minimal value sets, Pacific J. Math. 14 (1964) 225–241.

[12] G. Turnwald, A new criterion for permutation polynomials, Finite Fields Appl. 1 (1995) 64–82.
[13] D. Wan, A p-adic lifting lemma and its applications to permutation polynomials, in: Finite Fields, Coding Theory, and Advances in Communications and Computing, Las Vegas, NV, 1991, in: Lect. Notes Pure Appl. Math., vol. 141, Dekker, New York, 1993, pp. 209–216.
[14] D. Wan, J. Shiue, C. Chen, Value sets of polynomials over finite fields, Proc. Amer. Math. Soc. 119 (3) (1993) 711–717.